1. (currently amended) A service comprising:

determining that a mobile computer has lost connectivity to a first access point of a network;

when the mobile computer roams to a second access point of the network, determining whether the second access point is authorized for first secure communication and if so,

releasing access of the computer to first secure data on the network through the second access point, and otherwise releasing access of the computer to data other than the first secure data on the network through the second access point.

2. (original) The service of Claim 1, wherein the service is undertaken by the mobile computer.

3. (original) The service of Claim 2, wherein the service is undertaken by a hypervisor in the mobile computer.

4. (original) The service of Claim 1, wherein the service is undertaken by at least one network resource outside the mobile computer.

5. (original) The service of Claim 1, wherein the mobile computer is authenticated at the first access point, prior to losing connectivity thereto.

6. (original) The service of Claim 5 wherein releasing access to secure data on the network through the second access point comprises releasing access to a set of secure data which differs from the secure data released when the mobile computer is connected to the first access point.

7. (currently amended) A mobile computer, comprising:

at least one processor;

at least one wireless transceiver in communication with the processor, the processor executing logic including:

determining whether a predetermined communication hardware event has occurred; and

if a predetermined communication hardware event has occurred, selectively configuring the computer in a non-secure mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer.

8. (original) The computer of Claim 7, wherein the computer cannot access secure data on the network while configured in said non-secure mode.

9. (currently amended) The computer of Claim 7, wherein the computer can access a subset of the ~~secure~~ secure data on the network while configured in said non-secure mode.

10. (original) The computer of Claim 7, wherein the predetermined hardware event is a disconnection from a wireless access point.

11. (original) The computer of Claim 7, wherein the computer is configured in the non-secure mode if the computer roams to an access point that is not authorized for secure data transmission.

12. (original) The computer of Claim 10, wherein the processor accesses a list of authorized access points to undertake the act of selectively configuring.

13. (original) The computer of Claim 10, wherein the processor receives a network signal from a wireless access point to indicate whether the wireless access point is an authorized access point to undertake the act of selectively configuring.

14. (currently amended) A system including a mobile computer and a network including secure data, comprising:

means for determining that the mobile computer has lost connectivity to a first access point of the network;

means for determining whether a second access point of the network to which the mobile computer has roamed is authorized for secure communication; and

means for permitting the mobile computer to access secure data on the network through the second access point if the second access point is authorized for secure communication, and otherwise granting access to the computer to data other than the secure data through the second access point.

15. (original) The system of Claim 14, wherein the means are embodied in the mobile computer.

16. (original) The system of Claim 15, wherein the means are embodied by a hypervisor in the mobile computer.

17. (original) The system of Claim 14, wherein the means are embodied by at least one network resource outside the mobile computer.

18. (original) The system of Claim 14, wherein the mobile computer is authenticated at the first access point, prior to losing connectivity thereto.

19. (currently amended) A method comprising:

establishing communication between a mobile computer and a network through an access point; and

based on at least one of: a location, ~~and~~ or an identification, of the access point, ~~selectively~~ either granting the computer access to secure assets in the network or granting the computer access to other than the secure assets in the network.

20. (original) The method of Claim 19, wherein the act of selectively granting is undertaken by the mobile computer.

21. (original) The method of Claim 20, wherein the act of selectively granting is undertaken by a hypervisor in the mobile computer.

22. (original) The method of Claim 19, wherein the computer is configured to access a first set of network assets when communicating through a first access point and a second set of network assets when communicating through a second access point.